UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,602	07/30/2001	Christopher P. Jalbert	04860P2441	5216

7590 04/21/2006

EXAMINER
SCHUBERT, KEVIN R

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/21/2006

James C. Sheller
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,602	JALBERT ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-41 have been considered.

Allowable Subject Matter

Claims 7,18, and 28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6,12-13,17,19-22,24,26, and 34-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Vogelesang, U.S. Patent No. 5,953,424.

As per claims 1,20,21, and 22, the applicant describes a cryptographic method with the following limitations which are met by Vogelesang:

a) generating, at a first entity, a first public key M_B, the first entity having a first password P_B and the first public key M_B being session specific (Col 16, line 39 to Col 17, line 30);

b) receiving, at a first entity, a second public key M_A, the second public key M_A being session specific (Col 16, line 39 to Col 17, line 30);

a) generating, at the first entity, a first session key K_B based on the second public key M_A, the first public key M_B to be used at a second entity to derive the first session key, wherein the first session key K_B is independent of the first password P_B (Col 16, lines 39-42);

b) encrypting, at the first entity, a first random nonce N_B using at least the first password P_B and the public key M_A to obtain an encrypted random nonce (Col 16, lines 64-67);

c) transmitting the encrypted random nonce from the first entity to the second entity (Col 16, lines 64-67);

d) receiving a response to the encrypted random nonce (Col 17, lines 19-24);

e) authenticating through determining whether the response includes a correct modification of the first random nonce (Col 17, lines 28-30).

As per claim 2, the applicant describes the method of claim 1, which is met by Vogelesang, with the following limitations which are also met by Vogelesang:

a) generating a first secret S_B from at least the first password P_B and the first public key M_B (Col 16, lines 39-42);

b) encrypting the first random nonce N_B using at least the first secret S_B and the first session key K_B (Col 16, lines 64-67);

c) wherein the first secret S_B and the first session key K_B are different (Col 16, lines 64-67).

As per claims 3 and 4, the applicant describes the method of claim 1, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

Encrypting the first random nonce N_B using at least the first password P_B and the first session key K_B (Col 17, lines 25-37).

As per claim 5, the applicant describes the method of claim 1, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

a) generating a first random number R_B (Col 16, lines 39-40);

b) computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B, modulo a parameter B_B (Col 16, lines 39-42).

As per claim 6, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

Wherein the first secret S_B is generated using a combining function f_B on at least the first password P_B and the first public key M_B (Col 8, lines 7-10).

As per claims 12 and 13, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

Wherein the first random nonce is encrypted using a symmetrical encryption algorithm (Col 16, lines 64-67).

As per claims 17 and 19, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

a) generating a first random number N_B (Vogelesang: Col 13, lines 41-57);

b) encrypting a combination of the first random number N_B and the modified second random number (Vogelesang: Col 13, lines 41-57).

As per claims 24 and 38-40, the applicant describes a cryptographic method comprising the following limitations which are met by Vogelesang:

a) receiving at a first entity a second public key M_A and an encrypted second random number, the first entity having a password P_B (Vogelesang: Col 16, lines 33-38; lines 64-68);

b) generating a first session key K_B based on the second public key M_A, wherein the first session key K_B to retrieve a second random number N_A from the encrypted second random number (Vogelesang: Col 16, lines 39-42);

c) decrypting using at least a first password P_B and the first session key K_B to retrieve a second random number N_A from the encrypted second random number (Vogelesang: Col 17, lines 1-18);

d) modifying the second random number N_A to obtain a modified second random number (Vogelesang: Col 17, lines 19-24);

e) encrypting the modified second random number using at least the first password P_B and the first session key K_B to obtain an encrypted random package (Vogelesang: Col 7, lines 19-24; Schneier: pages 4-5);

f) transmitting the encrypted random package from the first entity (Vogelesang: Col 17, lines 25-27).

As per claim 26, the applicant describes the method of claim 24, which is met by Vogelesang, with the following limitations which are met by Vogelesang:

a) generating a first random number R_B (Col 16, lines 39-40);

b) computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B, modulo a parameter B_B (Col 16, lines 39-42).

As per claims 34-37, the applicant describes the method of claim 24, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

a) generating a first random number N_B (Col 16, line 33 to Col 17, line 27);

b) encrypting a combination of the first random number N_B and the modified second random number (Col 16, line 33 to Col 27, line 27).

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2,6,8-10,20-22, and 29-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone, U.S. Patent Application Publication No. 2001/0042205.

As per claims 1,20,21, and 22, the applicant describes a cryptographic method with the following limitations which are met by Vanstone:

a) generating, at a first entity, a first public key M_B, the first entity having a first password P_B and the first public key M_B being session specific ([0046]-[0062]);

b) receiving, at a first entity, a second public key M_A, the second public key M_A being session specific ([0046]-[0062]);

a) generating, at the first entity, a first session key K_B based on the second public key M_A, the first public key M_B to be used at a second entity to derive the first session key, wherein the first session key K_B is independent of the first password P_B ([0046]-[0062]);

b) encrypting, at the first entity, a first random nonce N_B using at least the first password P_B and the second public key M_A to obtain an encrypted random nonce ([0046]-[0062]);

c) transmitting the encrypted random nonce from the first entity to the second entity ([0046]-[0062]);

d) receiving a response to the encrypted random nonce ([0046]-[0062]);

e) authenticating through determining whether the response includes a correct modification of the first random nonce ([0046]-[0062]);

As per claims 2 and 6, the applicant describes the method of claim 1, which is met by Vanstone, with the following limitations which are also met by Vanstone:

a) generating a first secret S_B from at least the first password P_B and the first public key M_B (Vanstone: [0046]-[0062]);

b) encrypting the first random nonce N_B using at least the first secret S_B and the first session key K_B (Vanstone: [0046]-[0062]);

c) wherein the first secret S_B and the first session key K_B are different (Vanstone: [0046]-[0062]).

As per claims 8-10 and 29-31, the applicant describes the method of claims 2 and 28, which are met by Vanstone, with the following limitations which are also met by Vanstone:

a) combining the second public key M_A and the first public key M_B with the first password P_B to produce a first result (Vanstone: [0046]-[0062]);

b) hashing the first result with a secure hash (Vanstone: [0046]-[0062]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 14-16,25, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Schneier (Schneier, Bruce. Applied Cryptography. John Wiley & Sons. 1996. Washington DC. Pages 4-5 and 357).

As per claims 14-16,25, and 33, the applicant describes the method of claims 2 and 24, which are met by Vogelesang in view of Schneier, with the following limitation which is met by Schneier:

a) wherein encrypting the first random nonce N_B includes superencrypting the first random nonce N_B (Schneier: page 357);

Vogelesang discloses all the limitations of claims 2 and 24. However, Vogelesang fails to disclose superencrypting. Schneier discloses the use of superencrypting, which increases security in a system by adding another layer of encryption. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Vogelesang because doing so increases security in the system.

Claims 11,32, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Vanstone, U.S. Patent Application No. 2001/0042205.

As per claims 11 and 32, the applicant describes the method of claims 2 and 27, which are met by Vogelesang, with the following limitations which are also met by Vanstone:

a) combining the first password P_B and at least one of the second public key M_A and the first public key M_B to generate a first combined result (Vanstone: [0060]);

b) combining the first combined result and at least one of the second public key M_A, the first password P_B, and the first public key M_B to generate a second combined result (Vanstone: [0060]);

Vogelesang discloses all the limitations of claims 2 and 27. However, Vogelesang fails to disclose the particulars of the combination described above. Vanstone discloses combining variables in a similar fashion. It would have been obvious to one of ordinary skill in the art to combine the ideas of Vanstone with those of Vogelesang because doing so increases security in the system by enhancing complexity in the generation of variables.

As per claim 41, the applicant describes the method of claim 40, which is met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vogelesang:

Wherein the network is a network operating according to a hypertext transfer protocol and the first public key M_B is transmitted for session key exchange before the encrypted second random number is received (Col 1, lines 12-14; Col 16, lines 25-67).

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang.

As per claim 23, the applicant describes the system of claim 22, which is met by Vogelesang, with the following limitation:

A network operating according to a hypertext transfer protocol and the first public key M_B is transmitted with the encrypted random nonce for session key exchange (Col 1, lines 12-14);

Vogelesang does not disclose transmitting the first public key M_B with the encrypted random nonce. The examiner takes Applicant's failure to argue the previous official notice of the subject matter of claim 23 as acquiescence that the subject matter of claim 23 is obvious (See MPEP 2144.03). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to transmit a key with a nonce because doing so is more efficient than having to make two separation transmissions for the key and the nonce.

Response to Arguments

Applicant's arguments, see Remarks filed 3/21/06, with respect to the 102(b) rejection of claim 1 under Vogelesang have been fully considered but they are not persuasive. Applicant presents the following arguments:

1) Vogelesang does not anticipate part c) because S is dependent on K

2) Vogelesang does not anticipate part c) because a first public key is not used at a second entity to derive the first session key

Examiner respectfully disagrees with the above. Regarding 1), Applicant appears to be arguing that, in Vogelesang, a session key (e.g. S) may be based on an authentication factor (e.g. K) and hence Vogelesang does not disclose that a session key is independent of a password. Examiner respectfully notes that such expansive language as "a first password" does not limit the claim to any particular variable, such as K. Indeed, Examiner does not rely on K to meet Applicant's "a first password". Accordingly, Applicant's argument is moot.

Regarding 2), Applicant argues that a first public key is not used at a second entity to derive the first session key. Applicant offers no reasoning for such position. Examiner disagrees. Vogelesang discloses that two entities may each generate a public key (i.e. X,Y) and that the public keys may be sent to the other entity to derive a session key (S) (Col 16, lines 33-42). Accordingly, Examiner disagrees that Vogelsang fails to disclose that a first public key is used at a second entity to derive a first session key.

Applicant's arguments with respect to claim 2 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant's arguments with respect to the 102(b) rejection of claims 1-2,6-10,20-22,24-25,29-31, and 38-40 under Wu have been fully considered and are persuasive. The rejection of claims 1-2,6-10,20-22,24-25,29-31, and 38-40 has been withdrawn.

Applicant's arguments with respect to the 102(e) rejection of claims 1-2,6-10,20-22, and 29-31 under Vanstone fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant's arguments with respect to the 103(a) rejection of claim 24 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to the 103(a) rejection of claims 24 and 38-40 under Vogelesang in view of Vanstone have been fully considered but are not persuasive. Applicant presents the following arguments:

1) Vogelesang does not anticipate part b because S is dependent on K

2) Vanstone does not teach parts c through f

Examiner respectfully disagrees. Regarding 1), Examiner has previously addressed this issue in the instant action (see remarks with respect to the 102(b) rejection of claim 1 under Vogelesang). Regarding 2), Examiner submits that Vanstone is not relied on to teach, singly, parts c through f. Further, Examiner notes that Applicant's arguments, even if appropriate, are not in compliance with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention

without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER